

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 observing communication between a plurality of devices; and
3 inferring a respective state of at least one device of the plurality of devices based upon the
4 observing the communication.

1 2. The method of claim 1 wherein
2 the inferring is performed without sending a packet to the at least one device.

1 3. The method of claim 1 wherein
2 the inferring is performed without participating in the communication with the at least one
3 device.

1 4. The method of claim 1 wherein
2 the inferring is performed only by listening to the communication with the at least one device.

1 5. The method of claim 1 further comprising:
2 setting a designation for a first device of the plurality of devices to a threat when
3 the first device receives a packet and
4 the respective state of the first device is unfulfilled.

1 6. The method of claim 5 further comprising:
2 changing the designation for the first device to a non-threat when subsequent communication
3 initiated by the first device does not violate a rule for the communication.

1 7. The method of claim 1 further comprising:
2 setting a designation for a first device of the plurality of devices to a possible threat when
3 the communication is initiated by the first device, and
4 the communication initiated by the first device violates a rule.

1 8. The method of claim 7 further comprising:
2 changing the designation for the first device to a non-threat when subsequent communication
3 initiated by the first device does not violate a second rule for the communication.

1 9. The method of claim 1 further comprising:

2 setting a designation for a first device of the at least one device to a possible threat based
3 upon a packet configuration for a packet sent by the first device as part of the
4 communication.

1 10. The method of claim 1 wherein
2 the respective state of a first device of the at least one device is determined to be unknown.

1 11. The method of claim 10 wherein
2 the respective state of the first device is determined to be unknown when the observing the
3 communication comprises
4 observing that the first device fails to respond to the communication sent to the first
5 device.

1 12. The method of claim 1 wherein
2 the respective state of a first device of the at least one device is determined to be unfulfilled.

1 13. The method of claim 12 wherein
2 the respective state of the first device is determined to be unfulfilled when the observing the
3 communication comprises
4 observing an address resolution protocol request comprising a destination address for
5 the first device, and
6 observing that the first device does not respond to the address resolution protocol
7 request prior to expiration of a time limit.

1 14. The method of claim 12 wherein
2 the respective state of the first device is determined to be unfulfilled when the first device
3 receives an address resolution protocol request.

1 15. The method of claim 1 wherein
2 the respective state of a first device of the plurality of devices is determined to be used.

1 16. The method of claim 15 wherein
2 the respective state of the first device is determined to be used when the observing the
3 communication comprises
4 observing that the first device performs one of sending and receiving a packet.

1 17. The method of claim 15 wherein
2 the respective state of the first device is determined to be used when the observing the
3 communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device sent a reply to the packet within a time limit.

1 18. The method of claim 1 wherein
2 the respective state of a first device of the plurality of devices is determined to be virtual.

1 19. The method of claim 18 wherein
2 the respective state of the first device is determined to be virtual when the observing the
3 communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device did not send a reply to the packet within a time limit.

1 20. The method of claim 1 wherein
2 the respective state of a first device of the plurality of devices is determined to be automatic.

1 21. The method of claim 20 wherein
2 the respective state of the first device is determined to be automatic when
3 an automatic reply is programmed to be sent to a second address when the first device
4 receives a packet from the second address.

1 22. The method of claim 1 wherein
2 the respective state of the first device is determined to be omitted.

1 23. The method of claim 22 wherein
2 the respective state of the first device is determined to be omitted when
3 the observing is programmed to omit communication with the first device from the
4 observing.

1 24. The method of claim 1 further comprising:

2 initializing the respective state of at least one device of the plurality of devices to unknown
3 prior to the observing.

1 25. The method of claim 1 wherein
2 the plurality of devices communicates via a segment of a network.

1 26. The method of claim 1 further comprising:
2 maintaining the respective state for one device of the at least one device in a storage area.

1 27. The method of claim 1 wherein
2 storing information about at least one packet of a plurality of packets communicated between
3 the plurality of devices.

1 28. The method of claim 27 wherein
2 the information comprises a respective source address and a respective destination address for
3 each packet of the plurality of packets.

1 29. The method of claim 27 wherein
2 the information comprises a protocol for each packet of the plurality of packets.

1 30. The method of claim 27 wherein
2 the information comprises a time that each packet of the plurality of packets was sent.

1 31. A system comprising:
2 observing means for observing communication between a plurality of devices; and
3 inferring means for inferring a respective state of at least one device of the plurality of
4 devices based upon the observing the communication.

1 32. The system of claim 31 further comprising:
2 determining means for determining that the respective state is unknown when the observing
3 the communication comprises
4 observing that the first device fails to respond to the communication sent to the first
5 device.

1 33. The system of claim 31 further comprising:
2 determining means for determining that the respective state of the first device is unfulfilled
3 when the observing the communication comprises

4 observing an address resolution protocol request comprising a destination address for
5 the first device, and
6 observing that the first device does not respond to the address resolution protocol
7 request prior to expiration of a time limit.

1 34. The system of claim 31 further comprising:
2 determining means for determining that the respective state of the first device is unfulfilled
3 when the first device receives an address resolution protocol request.

1 35. The system of claim 31 further comprising:
2 determining means for determining that the respective state of the first device is used when
3 the observing the communication comprises
4 observing that the first device performs one of sending and receiving a packet.

1 36. The system of claim 31 further comprising:
2 determining means for determining that the respective state of the first device is used when
3 the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device sent a reply to the packet within a time limit.

1 37. The system of claim 31 further comprising:
2 determining means for determining that the respective state of a first device of the plurality of
3 devices is virtual when the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device failed to send a reply to the packet within a time limit.

1 38. The system of claim 31 further comprising:
2 determining means for determining that the respective state of the first device is automatic
3 when
4 an automatic reply is programmed to be sent to a second address when the first device
5 receives a packet from the second address.

1 39. The system of claim 31 further comprising:

2 determining means for determining that the respective state of the first device is omitted
3 when
4 the observing is programmed to omit communication with the first device from the
5 observing.

1 40. The system of claim 31 further comprising:
2 initializing means for initializing the respective state of at least one device of the plurality of
3 devices to unknown prior to the observing.

1 41. The system of claim 31 further comprising:
2 maintaining means for maintaining the respective state for one device of the at least one
3 device in a storage area.

1 42. The system of claim 31 further comprising:
2 storing means for storing information about at least one packet of a plurality of packets
3 communicated between the plurality of devices.

1 43. A system comprising:
2 an observing module configured to observe communication between a plurality of devices;
3 and
4 an inferring module configured to infer a respective state of at least one device of the
5 plurality of devices based upon the observing the communication.

1 44. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state is unknown when the
3 observing the communication comprises
4 observing that the first device fails to respond to the communication sent to the first
5 device.

1 45. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 unfulfilled when the observing the communication comprises
4 observing an address resolution protocol request comprising a destination address for
5 the first device, and

6 observing that the first device does not respond to the address resolution protocol
7 request prior to expiration of a time limit.

1 46. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 unfulfilled when the first device receives an address resolution protocol request.

1 47. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 used when the observing the communication comprises
4 observing that the first device performs one of sending and receiving a packet.

1 48. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 used when the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device sent a reply to the packet within a time limit.

1 49. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of a first device of the
3 plurality of devices is virtual when the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device failed to send a reply to the packet within a time limit.

1 50. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 automatic when
4 an automatic reply is programmed to be sent to a second address when the first device
5 receives a packet from the second address.

1 51. The system of claim 43 further comprising:
2 a determining module configured to determine that the respective state of the first device is
3 omitted when

4 the observing is programmed to omit communication with the first device from the
5 observing.

1 52. The system of claim 43 further comprising:
2 an initializing module configured to initialize the respective state of at least one device of the
3 plurality of devices to unknown prior to the observing.

1 53. The system of claim 43 further comprising:
2 a maintaining module configured to maintain the respective state for one device of the at least
3 one device in a storage area.

1 54. The system of claim 43 further comprising:
2 a storing module configured to store information about at least one packet of a plurality of
3 packets communicated between the plurality of devices.

1 55. A computer-readable medium comprising:
2 observing instructions configured to observe communication between a plurality of devices;
3 and
4 inferring instructions configured to infer a respective state of at least one device of the
5 plurality of devices based upon the observing the communication.

1 56. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state is unknown when
3 the observing the communication comprises
4 observing that the first device fails to respond to the communication sent to the first
5 device.

1 57. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of the first device is
3 unfulfilled when the observing the communication comprises
4 observing an address resolution protocol request comprising a destination address for
5 the first device, and
6 observing that the first device does not respond to the address resolution protocol
7 request prior to expiration of a time limit.

1 58. The computer-readable medium of claim 55 further comprising:

2 determining instructions configured to determine that the respective state of the first device is
3 unfulfilled when the first device receives an address resolution protocol request.

1 59. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of the first device is
3 used when the observing the communication comprises
4 observing that the first device performs one of sending and receiving a packet.

1 60. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of the first device is
3 used when the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device sent a reply to the packet within a time limit.

1 61. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of a first device of
3 the plurality of devices is virtual when the observing the communication comprises
4 observing that the first device received a packet when the respective state for the first
5 device was unfulfilled, and
6 observing that the first device failed to send a reply to the packet within a time limit.

1 62. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of the first device is
3 automatic when
4 an automatic reply is programmed to be sent to a second address when the first device
5 receives a packet from the second address.

1 63. The computer-readable medium of claim 55 further comprising:
2 determining instructions configured to determine that the respective state of the first device is
3 omitted when
4 the observing is programmed to omit communication with the first device from the
5 observing.

1 64. The computer-readable medium of claim 55 further comprising:

2 initializing instructions configured to initialize the respective state of at least one device of
3 the plurality of devices to unknown prior to the observing.

1 65. The computer-readable medium of claim 55 further comprising:
2 maintaining instructions configured to maintain the respective state for one device of the at
3 least one device in a storage area.

1 66. The computer-readable medium of claim 55 further comprising:
2 storing instructions configured to store information about at least one packet of a plurality of
3 packets communicated between the plurality of devices.